UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,543	03/01/2002	Peter M. Rigstad	3COM-3828.MCD.US.P	5432

7590 03/17/2005

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, CA 95113

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,543	RIGSTAD ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25,32-34 and 36-39* is/are rejected.

7)☒ Claim(s) *26-31 and 35* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment on 28 January 2005.

2. Claims 1-39 are pending in the application.

3. Claims 26-31 and 35 have been objected to.

4. Claims 1-25, 32-34 and 36-39 have been rejected.

Response to Amendment

5. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

Response to Arguments

6. Applicant's arguments with respect to claims 1-39 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 4-6, 10, 12, 13, 15-20, 22-24, 32, 33, 36 and 39 rejected under 35 U.S.C. 103(a) as being unpatentable over Antur et al et al U.S. Patent No. 6,243,815 B1 in view of Boswell, Jr. et al U.S. Patent No. 6,272,169 B1 (hereinafter Boswell).

As to claims 1, 22 and 36, Antur et al discloses a system for providing a firewall to a communication device, the system comprising:

a first device comprising a hardware implemented firewall [column 9, lines 10-36], the first device coupled to a host device that is coupled to the communication device for establishing a connection to a network [column 7, lines 12-23]; and

the logic on the system configured to cause data transferred by the communication device to be processed by the firewall on the first device [column 9, lines 10-36].

Antur et al does not teach:

logic residing in the system other than on the communication device, the logic allowing the communication device to establish a connection to the network, wherein the logic further allows the host device to connect to the network using the communication device, wherein neither the host device nor the communication device has a firewall capability that is required by the network to connect to the network.

Boswell teaches:

logic residing in the system (i.e. host computer) other than on the communication device (i.e. software modem), the logic allowing the communication device to establish a connection to the network, wherein the logic further allows the host device to connect to the network using the communication device, wherein neither the host device nor the communication device has a firewall capability that is required by the network to connect to the network [column 2, lines 47-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Antur et al so that the hardware modem on the host computer would have been replaced by the software modem as taught by Boswell. It would have been the logic on the host computer that would have allowed the software modem to establish a connection to the network. Neither the host computer nor the software modem would have had any firewall capabilities.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Antur et al by the teaching of Boswell because software designs may be more easily changed than hardware designs. Likewise, it may be easier to update the software designs and to provide the updates to users [column 1, lines 24-40].

As to claim 4, Antur et al teaches a server for providing policies to be used by the firewall and that the first device is operable to access the server to receive the policies [column 6, lines 50-59].

As to claim 5, Antur et al teaches that the system further comprises a plurality of nodes having a hardware-implemented firewall [column 9, lines 10-14]. Antur et al teaches that the server is further operable to transfer the policies to the plurality of nodes and that the system comprises a centrally managed network having nodes with hardware implemented firewalls [column 9, lines 45-61].

As to claim 6, Antur et al teaches that the logic to allow the system to establish a connection to the network comprises hardware implemented token [column 5, lines 42-53].

As to claim 10, Antur et al teaches logic for preventing login of the host device unless the first device is coupled to the host device [column 6, lines 11-17].

As to claim 12, Antur et al teaches that the first device is physically coupled to the communication device [column 7, lines 12-23]. Antur et al teaches that the data transferred by the communication device to the network is processed by the firewall before it is transferred into the network and the data transferred from the network to the communication device passes through the firewall before it reaches the host device [column 9, lines 10-36].

As to claim 13, Antur et al teaches that the physical connection is of the same medium as the network connection [column 7, lines 12-23].

As to claim 15, Antur et al teaches that the system further comprises a software driver in the host device and that the driver is operable to pass data that is received by the communication device to the first device to be processed by the firewall [column 7, lines 12-23].

As to claim 16, Antur et al teaches that the software driver is further operable to pass data which is to be transferred by the communication device over the network to the first device to be processed by the firewall, as discussed above.

As to claim 17, Antur et al teaches a software component installed above a driver for the communication device, the software component operable to route data for the communication device to the first device [column 7, lines 12-23].

As to claim 18, Antur et al discloses that the software component is a shim that resides above a miniport driver [column 7, lines 12-23].

As to claim 19, Antur et al teaches a software component installed below a driver for the communication device and that the software component is operable to route data for the communication device to the first device [column 7, lines 12-23].

As to claim 20, Antur et al teaches transfer security logic residing on the first device. Antur et al teaches that the transfer security logic is for securely transferring data between the first device and a server in the network [column 7, lines 29-35].

As to claims 23 and 33, Antur et al teaches that the host device routes the data to the firewall device is to be processed by the hardware-implemented firewall, as discussed above. Antur et al teaches that the routing takes place at a physical layer in the data stack [column 4, lines 35-57].

As to claim 24, Antur et al teaches sending policies to the firewall device and that the operation of the hardware implemented firewall is modified [column 6, lines 50-59].

As to claim 32, Antur et al teaches transferring data to be transferred over the network by the communication interface device to the firewall device, as discussed above. Antur et al teaches processing the data with the hardware-implemented firewall, as discussed above. Antur et al teaches that the data is processed by the hardware-implemented firewall before it is transferred over the network connection established via the communication interface device, as discussed above.

As to claim 39, Antur et al teaches that the hardware-implemented firewall is dedicated to the host device [column 6, lines 60-67].

8. Claims 2, 8, 9, 11, 21, 25 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Antur et al et al U.S. Patent No. 6,243,815 B1 and Boswell, Jr. et al U.S. Patent No. 6,272,169 B1 as applied to claims 1 and 22 above, and further in view of Gleichauf et al U.S. Patent No. 6,324,656 B1.

As to claims 2, 11 and 25, the Antur-Boswell combination does not teach logic for checking integrity of software components in the system.

Gleichauf teaches logic for checking integrity of software components in the system. Gleichauf teaches that network devices are scanned for the potential vulnerabilities inherent to the services and the operating system of each device [column 5, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination so that the computer implemented firewall would have performed a scan for the potential vulnerabilities to the services and the operating system for each device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination by the teaching of Gleichauf is that each device connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

As to claim 8, the Antur-Boswell combination does not teach an alert log for logging possible breaches detected by the system.

Gleichauf teaches an alert log for logging possible breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination so that the computer implemented firewall would have performed a scan for the potential vulnerabilities and stored the potential vulnerabilities in a database.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination by the teaching of Gleichauf because it confirms identified potential vulnerabilities [column 2, lines 55-56].

As to claim 9, Gleichauf teaches a configuration integrity checker (i.e. NVA engine **20**) for checking integrity of software components (i.e. operating system) in the system, wherein the possible breach is detected by the configuration integrity checker [Gleichauf column 5, lines 41-45].

As to claims 21 and 34, the Antur-Boswell combination teaches server for providing policies to be used by the firewall, as discussed above.

The Antur-Boswell combination does not teach a configuration integrity checker for checking integrity of software components in the system. The Antur-Boswell combination does not teach an alert log for logging possible security breaches detected by the system.

Gleichauf teaches a configuration integrity checker for checking integrity of software components in the system. Gleichauf combination teaches a configuration integrity checker (i.e. NVA engine **20**) for checking integrity of software components (i.e. operating system) in the system. Gleichauf teaches that the possible breach was detected by the configuration integrity checker [column 5, lines 41-45]. Gleichauf teaches an alert log for logging possible breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49]. Gleichauf teaches an alert log for logging possible security breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination so that an NVA engine would have been included on the computer that the firewall resides. The NVA would have scanned the software components of the devices on the network and recorded a log for possible security breaches. The server of the Antur-Boswell combination would have provided the policies for the NVA engine.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination by the teaching of Gleichauf is that each device connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

9. Claims 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Antur et al et al U.S. Patent No. 6,243,815 B1 and Boswell, Jr. et al U.S. Patent No. 6,272,169 B1 as applied to claim 1 above, and further in view of Servi U.S. Patent No. 5,278,904.

As to claim 7, the Antur-Boswell combination teaches that the second device is coupled to the first device, as discussed above.

The Antur-Boswell combination does not teach a second device having stored thereon data needed to establish the connection to the network. The Antur-Boswell combination does not teach logic to allow the system to establish the connection and is operable to access the data to assure the first device must be in the system to establish the connection to the network via the communication device

Servi teaches a stored password on a requesting node to access protected resources on a server node [column 1, lines 55-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination so that any of the firewall devices would have been authenticated by a stored password to receive policies from the security policy server. The password would have been stored data used to establish the connection to the network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination is that this provides a method for reliable identification of a device attempting access to protected resources by a remote verifier using reduced communications [column 1, lines 45-47].

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Antur et al et al U.S. Patent No. 6,243,815 B1 and Boswell, Jr. et al U.S. Patent No. 6,272,169 B1 as applied to claim 1 above, and further in view of Dempsey et al U.S. Patent No. 5,826,048.

As to claim 14, the Antur-Boswell combination does not teach that the physical connection comprises an MPCI (Mini Peripheral Component Interconnect) adapter to couple the first device to the communication device.

Dempsey teaches a MPCI interface for connecting a PCI bus to one or more external devices [column 2, lines 43-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination so that the MPCI interface would have connected the firewall to the NIC.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination by the teaching of

Dempsey because it reduces the number of signals required in implementing a PCI compliant interface by multiplexing and subsequently de-multiplexing signals. It also can be used to interface non-PCI devices and bus, and can be adapted or modified to reduce the number of pins/signals associated with these devices and buses [column 3, lines 51-58].

11. Claims 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Antur et al et al U.S. Patent No. 6,243,815 B1 and Boswell, Jr. et al U.S. Patent No. 6,272,169 B1 as applied to claim 36 above, and further in view of Fischer U.S. Patent No. 5,475,826.

As to claim 37, the Antur-Boswell combination does not teach logic for performing a configuration integrity check of software component. The Antur-Boswell combination does not teach that the logic is operable to produce a numeric value that results from the check. The Antur-Boswell combination does not teach a stored value for each software component to be checked for integrity. The Antur-Boswell combination does not teach logic to compare the produced value with the stored value.

Fischer teaches it is well known that file integrity is protected by taking a one-way hash (e.g., by using MD5 or the secure hash algorithm SHA) over the contents of the file. By implementing and checking a currently computed hash value, with a previously stored hash value, correct file integrity assures the threat of malicious tampering (or even accidental external modification) can be detected--thereby improving the reliability and security of ultimate results. Assuming it is stored in a way that preserves its own integrity, the file hash can be used to insure that the entire file has not been damaged or deliberately tampered [column 1, lines 37-47].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination so that a hash on

the software component is done to produce a hash value and compared with a stored hash value on the firewall to perform the configuration integrity check.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination by the teaching of Fischer because massive re-computation for each file alteration, long periods in which the file is in jeopardy of being considered "invalid" if the application or system is abruptly terminated, additional storage space for a hash (or MAC) for each record, and the ability of an adversary to substitute stale records because the integrity of the entire file, and the inter-relationship of all records is maintained encapsulated in a single file HASH value which changes as each file update is performed [column 3, lines 48-57].

12. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Antur et al et al U.S. Patent No. 6,243,815 B1 and Boswell, Jr. et al U.S. Patent No. 6,272,169 B1 as applied to claim 36 above, and further in view of Servi U.S. Patent No. 5,278,904.

As to claim 38, the Antur-Boswell combination teaches that a user would have to provide proof that he is authorized to initiate a connection [column 11, lines 4-21]

The Antur-Boswell combination does not teach that the first logic comprises stored values to be used in an authentication process during establishment of the network connection.

Servi teaches a stored password on a requesting node to access protected resources on a server node [column 1, lines 55-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the Antur-Boswell combination so that any of the

firewall devices would have been authenticated by a stored password to establish a network connection.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Antur-Boswell combination by the teaching of Servi because this provides a method for reliable identification of a device attempting access to protected resources by a remote verifier using reduced communications [column 1, lines 45-47].

Allowable Subject Matter

13. Claims 26-31 and 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As to claim 26, prior art does not teach or fairly disclose that the configuration integrity check is performed before the network connection is allowed and the connection is allowed only if the configuration integrity check passes.

As to claim 27, prior art does not teach or fairly disclose performing a hash on the software component to produce a hash value and comparing the hash value with a stored hash value to perform the configuration integrity check.

As to claim 28, prior art does not teach or fairly disclose that the stored hash value resides on the firewall device.

As to claims 29 and 35, prior art does not teach or fairly disclose sending an alert if the configuration integrity check fails.

As to claim 30, prior art does not teach or fairly disclose storing an alert if the configuration integrity check fails.

As to claim 31, prior art does not teach or fairly disclose swapping resource spaces in the host device that are reserved for the communication interface device and the firewall device.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
March 9, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100